

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è UTILIZZARE PROPRIAMENTE L'ANALISI DELLE DIGITAL EVIDENCES, DARIO FORTE, IN CIBERSPAZIO E DIRITTO, 2000, VOLUME I, NUMERO IV, PP. 537-543. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

Utilizzare propriamente l'analisi delle 'Digital Evidences'

Dario Forte

1. L'aiuto dato dall'analisi comportamentale.

Questa tecnica viene denominata 'Behavioral evidence analysis'. Dato per assunto un processo corretto di acquisizione delle *digital evidences*, risulta necessario effettuare una correlazione tra i dati acquisiti e *modus operandi*, al fine di restringere il campo d'azione.

Ecco una prima suddivisione in macro categorie cui può essere d'aiuto l'analisi comportamentale:

1. definire un primo *pool* generale di sospetti. A seconda dei movimenti effettuati e dello 'stile' utilizzato per l'intrusione, nonché della sua potenziale provenienza (solitamente si parte da una prima suddivisione di quest'ultima tra interno ed esterno) l'operatore può iniziare una prima scrematura. Questa metodica potrà essere di maggiore ausilio nel caso di intrusione accertata da parte di una risorsa interna. In questo caso, infatti, il cosiddetto 'suspect pool' sarà sufficientemente ristretto;
2. comprendere le eventuali ragioni dell'avvenuto attacco. A seconda della risorsa colpita, delle eventuali azioni intraprese dopo il successo dell'intrusione ed altre informazioni acquisite, si può iniziare una prima definizione delle motivazioni che hanno spinto i soggetti attivi del reato. Se, per esempio, viene effettuato un *defacement* (modifica totale o parziale di grafica/testo o, comunque, contenuti di una pagina *Web*), a seconda del messaggio che solitamente appare sulla pagina si può tentare un primo inquadramento. Un caso pratico, in questo caso, è dato dal *defacement* effettuato nei confronti del sito della Nike (www.nike.com). In quel caso gli *attacker* hanno lasciato un messaggio esplicito contro la WTO ed una promessa di ritornare a sferrare un nuovo e duro attacco. Una violazione di questo tipo potrebbe far pensare ad atti di valenza ideologica, al contrario, invece, della recente intrusione effettuata nel *network* di Microsoft che, stando alle ultime notizie ufficiali, avrebbe consentito il furto di grosse porzioni di codice sorgente di Sistemi Operativi ed applicazioni di produttività; in questo caso il movente dell'attacco è evidentemente di natura spionistico industriale. Alla stessa stregua, si possono circoscrivere eventuali atti compiuti dai cosiddetti *Script Kiddies*, cioè da personaggi che non hanno un vero e proprio *skill* consolidato e che acquisiscono strumenti scritti da terzi, li 'customizzano' e li utilizzano per i loro fini. A volte gli attacchi portati a termine da questa tipologia di persone possono essere privi dei fondamenti di cui abbiamo appena parlato. Tuttavia la mancanza di una motivazione ideologica o tecnica, non può (e non deve) costituire un'attenuante per il soggetto attivo del reato;

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Ciberspazio e Diritto" (<http://www.ciberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è UTILIZZARE PROPRIAMENTE L'ANALISI DELLE DIGITAL EVIDENCES, DARIO FORTE, IN CIBERSPAZIO E DIRITTO, 2000, VOLUME I, NUMERO IV, PP. 537-543. Articolo tratto dal sito <http://www.ciberspazioediritto.org>

3. effettuare le giuste 'interviste' e i giusti interrogatori. Le prime sono quelle che si effettuano all'interno della struttura, al fine di raggiungere la massima comprensione di quello che è accaduto, mentre i secondi sono quelli effettuati nei confronti degli indagati;

4. comprendere gli errori effettuati dal *security management*. Come più volte stabilito in letteratura, uno dei compiti delle procedure di *incident handling*, consiste nel comprendere gli errori effettuati nel gestire la sicurezza delle strutture compromesse. L'analisi comportamentale può sicuramente essere d'aiuto nell'individuazione di eventuali sbagli e per non ripetere gli stessi.

L'analisi comportamentale non richiede, come alcuni potrebbero supporre, uno *skill* prevalentemente basato sulla psicologia. Come la stessa letteratura introduttiva sulla materia ha più volte affermato, l'analisi si basa su un processo di verifica a 360 gradi della notizia acquisita. Partendo da questa prima analisi si giungerà ad una successiva correlazione tra gli elementi descritti poc'anzi.

2. Verificare i falsi allarmi¹ e gestire le informazioni acquisite.

Uno dei primi spunti che l'analisi comportamentale è in grado di fornire è l'aiuto nella determinazione dei falsi allarmi. Spesso, infatti, può verificarsi un evento, per esempio causato da un impiegato interno, che, nonostante tecnicamente possa indicare un tentativo di violazione, è in realtà da ridimensionare dal punto di vista pratico.

Trattandosi di una disciplina basata fondamentalmente sull'interpretazione degli eventi, per far sì che quest'ultima sia caratterizzata dall'univocità di cui sopra, bisognerà innanzitutto stabilire un unico *team* che si occupi dell'analisi. Questo perché la metodica di interpretazione deve essere la stessa dall'inizio alla fine dell'indagine. Questo è un concetto molto importante soprattutto nella fase di *equivocal forensic analysis*.

Questa è una disciplina correlata a qualsiasi dato soggetto ad interpretazione o aperto a più di una valutazione.

Importanza fondamentale nell'applicazione dell'*equivocal forensic analysis* è data alle 'interviste' da effettuare nei confronti dei potenziali soggetti coinvolti.

La sinergia delle attività di cui sopra, unita a quella di analisi convenzionale sulle fonti di prova fisico/virtuali (*digital and physical forensic*) può dare spesso luogo ad una vera e propria definizione di *pattern* comportamentali ben definiti. Questi possono servire sia per l'investigazione nella quale si sta operando sia per i lavori futuri. Una cosa

¹ L'accezione di falso allarme che utilizziamo in questa sede è di tipo globale. Nel gergo tecnico, infatti, specie nell'*intrusion detection* e nelle attività correlate, falso allarme è indicativo di una errata interpretazione di un evento. In questo caso, invece, all'interpretazione dell'evento va aggiunta quella delle circostanze oggettive ad esso inerenti.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è UTILIZZARE PROPRIAMENTE L'ANALISI DELLE DIGITAL EVIDENCES, DARIO FORTE, IN CIBERSPAZIO E DIRITTO, 2000, VOLUME I, NUMERO IV, PP. 537-543. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

costruttiva potrebbe essere la creazione di un *database* comportamentale relativo alle metodiche adottate nel corso degli attacchi. Una linea guida (forse utopica) di implementazione potrebbe essere la seguente:

1. creazione del *database*. Il modello di analisi e sviluppo potrebbe essere definito a livello internazionale da una commissione di operatori. Detti operatori, appartenenti alle varie nazioni di provenienza, ed appartenenti al mondo accademico, aziendale e, ovviamente, giudiziari, devono dimostrare di aver acquisito un'esperienza operativa basata su casi reali (anche se non risolti) a cui hanno partecipato. Ci troviamo in una situazione paradossale in cui esiste una comunità di operatori e consulenti che lavorano su casi reali, un'altra di teorici ed operativi che fa giusta divulgazione, ed un'altra, solo di teorici che vengono chiamati come consulenti, pagati fior di Euro per rilasciare consulenze piene di elucubrazioni senza alcun riscontro pratico. In poche parole: fiumi di parole inutilizzabili nel mondo reale. Il problema maggiore è che dette consulenze spesso si tramutano in norme, e questo non va bene.

2. aggiornamento del *database* da effettuarsi a cura degli investigatori. Il flusso delle informazioni potrebbe essere il seguente:

il *response team* aziendale o il suo *security management*, inizializzano la fase del *green circle*, colloquiando con l'autorità investigativa. Gli operatori della Polizia Giudiziaria, di concerto con il *team* di cui sopra, gestiscono una procedura univoca di catalogazione delle *digital evidences*, secondo le linee guida sopra citate; a caso chiuso, se concesso dalla competente Autorità Giudiziaria, la catalogazione delle *evidences* viene trasferita nel *database* centrale.

L'immissione dei dati dovrebbe essere a cura del Reparto operante della Polizia Giudiziaria. Questo potrebbe, a sua volta, conservare le generalità dell'azienda colpita, lasciando nel *database* soltanto le informazioni necessarie ad inquadrare eventuali coincidenze. In questo modo si tutelerebbe ulteriormente la riservatezza del cosiddetto *target owner*. La consultazione del *database* sarebbe riservata agli stessi operatori di Polizia, debitamente autorizzati.

3. La vittimologia come strumento di ausilio alla Computer Forensic.

Una verifica iniziale comprende l'individuazione delle macchine compromesse. Una volta fatto ciò bisogna verificare che tipo di violazione sia stata effettuata e quali siano stati i passi fatti per compierla. Quanti più saranno gli eventi riconducibili ad una violazione tanto più si potrà parlare di circostanze inequivocabili. L'applicazione dell'analisi comportamentale è susseguente alla fase di cui abbiamo appena parlato. Ad essa va affiancata un'altra disciplina chiamata vittimologia, che si occupa di definire le caratteristiche generali dell'entità colpita dall'attacco. Una propria applicazione dello studio vittimologico può dare degli elementi valutativi sulle motivazioni che possono aver portato all'effettuazione dell'attacco; lo studio delle *policy* di utilizzo e di gestione delle *permission* può far comprendere le eventuali falle di

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è UTILIZZARE PROPRIAMENTE L'ANALISI DELLE DIGITAL EVIDENCES, DARIO FORTE, IN CIBERSPAZIO E DIRITTO, 2000, VOLUME I, NUMERO IV, PP. 537-543. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

cui l'*intruder* può aver approfittato. Inoltre può portare altresì all'individuazione di eventuali errori in sede di amministrazione, dovuti a dolo o colpa grave.

Riconducibile alle attività vittimologiche è la verifica dei possibili rapporti intercorrenti tra il *target owner* ed i potenziali sospetti. Stabilire i possibili collegamenti è davvero utile. Un tentativo per arrivare a ciò potrebbe essere fatto individuando (cronologicamente ed effettivamente) la fase di *information gathering* (acquisizione delle informazioni sull'obiettivo). È questa una delle fasi più importanti di tutta l'analisi. Molto spesso, infatti, riconoscere l'attività di 'investigazione' effettuata dal nemico può essere utile sia per l'individuazione del nemico stesso, sia dei *target* che questo aveva in programma di compromettere.

4. Il ruolo del risk analysis/assessment.

Nell'applicazione delle pratiche vittimologiche ampia attenzione va prestata nell'analizzare le procedure di *risk analysis/assessment*. Questo riveste importanza fondamentale in quanto, come detto prima, contribuisce ulteriormente alla definizione del quadro del *target* e, consequenzialmente, del potenziale *range* di sospetti.

Allo stato attuale viene effettuata una suddivisione di tre macrocategorie:

1. rischio del *target* (*target risk*): in questo caso si intende il rischio cui è sottoposta una particolare risorsa (*host*) situata all'interno della struttura. Alcuni tendono a definire l'importanza del rischio proporzionalmente al fatto che la macchina si trovi protetta o meno da un *firewall* o altri prodotti. In realtà non tutti sono d'accordo con questa qualificazione;
2. rischio della vittima (*victim risk*): in questo caso l'accezione è relativa alla struttura tutta, quindi posizione aziendale, immagine, valenza della ricerca e sviluppo, piano *marketing* e via dicendo. La qualificazione viene calcolata altresì in base all'esposizione aziendale, con particolare attenzione nei confronti di eventuali posizionamenti pubblici (quotazioni);
3. rischio dell'*attacker* (*offender risk*): quanto l'*attacker* è in grado di mascherare la sua attività? Quanto l'infrastruttura di sicurezza è in grado di tracciare l'autore della violazione? In questa accezione dell'*offender risk* la qualificazione del grado di rischio è data dall'applicabilità della formula $Pt > Dt + Rt$, riconducibile al concetto di *Time Based Security*, di cui si tratterà in un prossimo articolo.